

FINAL PROJECT
COMPARISON OF SHORT RANGE
WIRELESS NETWORKS (PAN's)

ZigBee vs. Bluetooth



Course: Mobile Communication and Networks

Date: 1st June 2011



Dedication

I dedicate this project to myself, dear parents
and sisters who were a great support.

Acknowledgement

First of all I thank ALLAH, the Almighty, for bestowing me with determination and grit to undergo the project. I owe my gratitude to many people for the guidance they endowed me with. Foremost on the list is Ms Jaweria Malik, my supervisor, who was sheer source of guidance and encouragement. I am also gratified to my family whose suggestions have helped me to improve and render this project

Abstract

In this research report we have done a comparative study of Bluetooth and zigbee. Both are the short range wireless technologies (PAN's). But in this research report we try to explain the working of both the technologies and their comparison too. With time as all the technologies get developed then how these short range devices make their own place in the world of technology. And the full overview of both technologies and their comparison.

Table of Contents

Sr. no	Content	Page No
1	<u>ZigBee</u>	6
2	Introduction.....	6
3	How zigbee works.....	7
4	ZigBee Network Topologies.....	8
5	How ZigBee Operates.....	9
6	What zigbee do.....	9
7	<u>BLUETOOTH</u>	11
8	Introductioon.....	11
9	How Bluetooth Creates a Connection	12
10	How Bluetooth Operates.....	13
11	Bluetooth Pico nets	14
12	Bluetooth Security	16
13	Difference between ZigBee and Bluetooth.....	17
14	Conclusion.....	20

ZigBee: -

Introduction:

ZigBee is a technological standard, based on the IEEE 802.15.4 standard, which was created specifically for control and sensor networks. Within the broad organization of the Institute of Electrical and Electronics Engineers (IEEE), the 802 group is the section that deals with network operations and technologies. Group 15 works more specifically with wireless networking, and Task Group 4 drafted the 802.15.4 standard for a low data rate wireless personal area network (WPAN). The standard for this WPAN specifies not only a low data rate but also low power consumption and low complexity, among other things. The data rate is limited to 250 kbps in the global 2.4 GHz Industrial, Scientific, Medical (ISM) band, 20 kbps in the 868 MHz band used in Europe, and 40 kbps in the 915 MHz band used in North America and Australia. The ZigBee standard is built on top of this IEEE standard, addressing remote monitoring and control for sensory network applications. This standard was created by an organization known as the ZigBee Alliance, which is composed of a large number of companies and industry leaders striving to enable such control devices based on said standard. Figure 1 below shows the relationship between IEEE 802.15.4 and ZigBee.

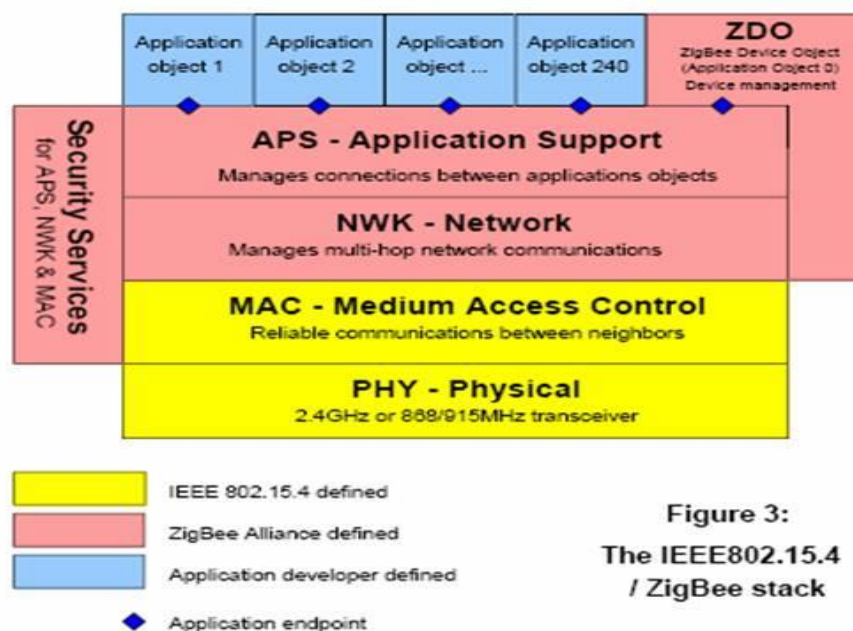


Figure 3:
The IEEE802.15.4
/ ZigBee stack

Figure 1: ZigBee Stack Architecture

As can be seen in the figure, IEEE 802.15.4 develops the Medium Access Control (MAC) Layer and Physical (PHY) Layer, which address such things as the frequency and data rate specifications. The Physical Layer also allows for two types of devices: full function devices (FFD's) and reduced function devices (RFD's). ZigBee, meanwhile, develops the Network Layer and Application Layer, which includes the Applications Support Sublayer, the ZigBee Device Object, and the Security Services. The Network Layer and Application Layer are more specific than the IEEE layers and involve such things as how a ZigBee network is to be set up, how the devices in the network relate to one another, and so on.

How ZigBee Works:

ZigBee basically uses digital radios to allow devices to communicate with one another. A typical ZigBee network consists of several types of devices. A network coordinator is a device that sets up the network, is aware of all the nodes within its network, and manages both the information about each node as well as the information that is being transmitted/received within the network. Every ZigBee network must contain a network coordinator. Other Full Function Devices (FFD's) may be found in the network, and these devices support all of the 802.15.4 functions. They can serve as network coordinators, network routers, or as devices that interact with the physical world. The final device found in these networks is the Reduced Function Device (RFD), which usually only serve as devices that interact with the physical world. An example of a ZigBee network is shown below in Figure 2.

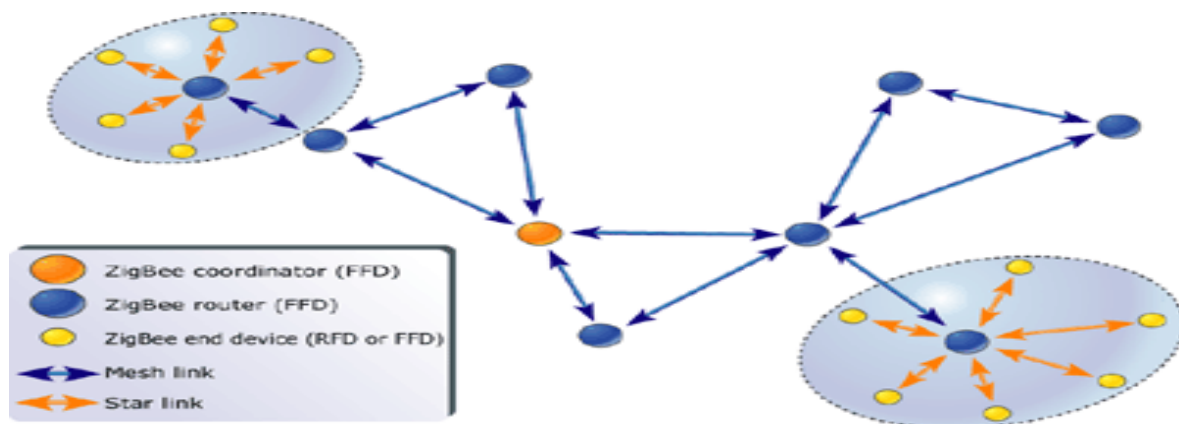


Figure 2: ZigBee Network

The figure above introduces the concept of the ZigBee network topology.

ZigBee Network Topologies:

Several topologies are supported by ZigBee, including star, mesh, and cluster tree. Star and mesh networking are both shown in the figure above. As can be seen, star topology is most useful when several end devices are located close together so that they can communicate with a single router node. That node can then be a part of a larger mesh network that ultimately communicates with the network coordinator. Mesh networking allows for redundancy in node links, so that if one node goes down, devices can find an alternative path to communicate with one another. Figures 3 and 4 below provide an example of how mesh networking allows for multiple paths between devices.

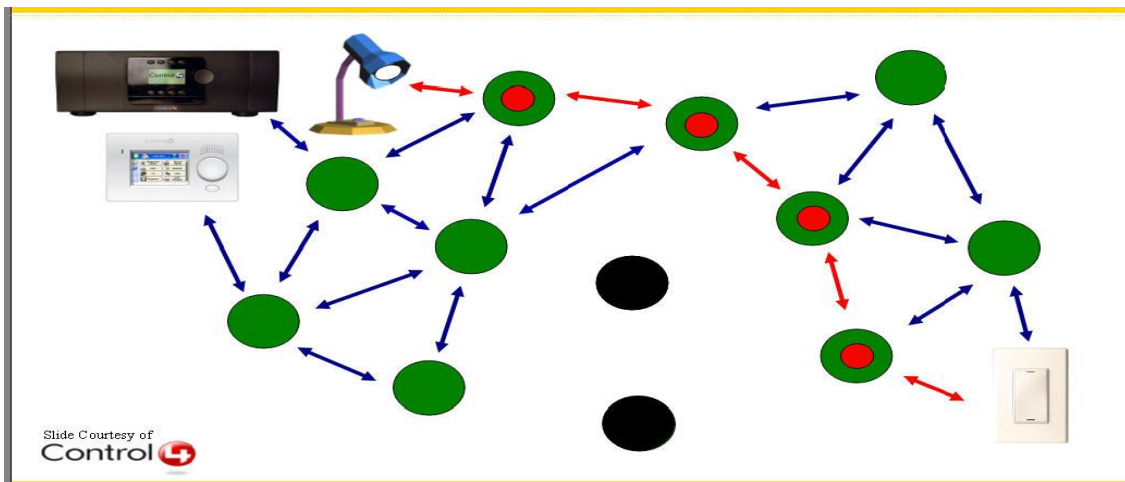


Figure 3: Mesh Networking Path 1

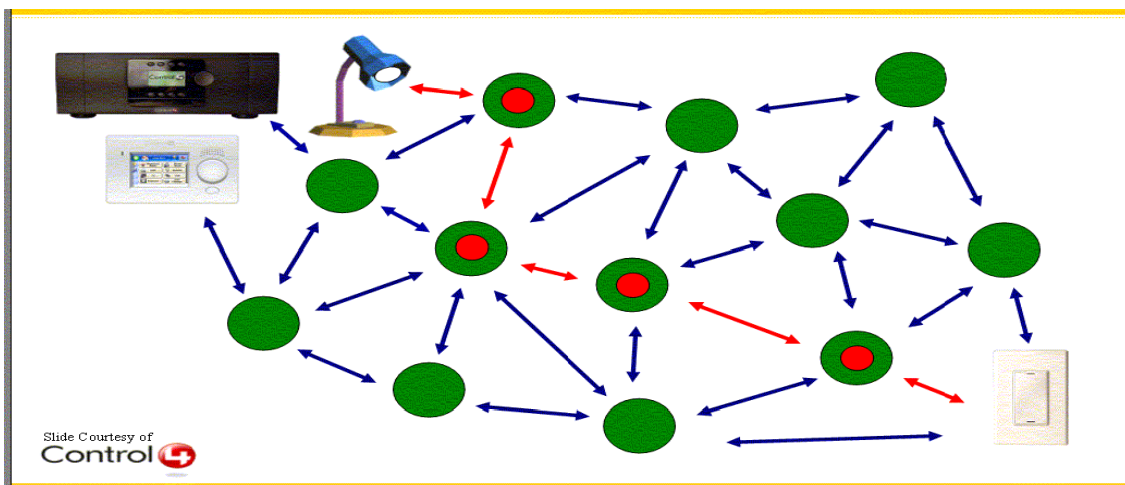


Figure 4: Mesh Networking Path 2

How ZigBee Operates:

ZigBee operates in two main modes: non-beacon mode and beacon mode. Beacon mode is a fully coordinated mode in that all the devices know when to coordinate with one another. In this mode, the network coordinator will periodically "wake-up" and send out a beacon to the devices within its network. This beacon subsequently wakes up each device, who must determine if it has any message to receive. If not, the device returns to sleep, as will the network coordinator, once its job is complete. Non-beacon mode, on the other hand, is less coordinated, as any device can communicate with the coordinator at will. However, this operation can cause different devices within the network to interfere with one another, and the coordinator must always be awake to listen for signals, thus requiring more power. In any case, ZigBee obtains its overall low power consumption because the majority of network devices are able to remain inactive over long periods of time.

What Does ZigBee Do:

ZigBee is designed for wireless controls and sensors. It could be built into just about anything you have around your home or office, including lights, switches, doors and appliances. These devices can then interact without wires, and you can control them all. Although ZigBee's underlying radio-communication technology isn't revolutionary, it goes well beyond single-purpose wireless devices, such as garage door openers and "The Clapper" that turns light on and off. It allows wireless two-way communications between lights and switches, thermostats and furnaces, hotel-room air-conditioners and the front desk, and central command posts. It travels across greater distances and handles many sensors that can be linked to perform different tasks.

ZigBee works well because it aims low. Controls and sensors don't need to send and receive much data. ZigBee has been designed to transmit slowly. It has a data rate of 250kbps (kilobits per second), pitiful compared with Wi-Fi, which is hitting throughput of 20Mbps or more. But because ZigBee transmits slowly, it doesn't need much power, so batteries will last up to 10 years. Because ZigBee consumes very little power, a sensor and transmitter that reports whether a door is open or closed, for example, can run for up to five years on a single double-A battery. Also, operators are much happier about adding ZigBee to their phones than faster technologies such as Wi-Fi; therefore, the

phone will be able to act as a remote control for all the ZigBee devices it encounters. Figure 5 below gives a great example of how ZigBee can be applied.



Figure 5: ZigBee Application

BLUETOOTH: -

Introduction:

When you use computers, entertainment systems or telephones, the various pieces and parts of the systems make up a community of electronic devices. These devices communicate with each other using a variety of wires, cables, radio signals and infrared light beams, and an even greater variety of connectors, plugs and protocols.

There are lots of different ways that electronic devices can connect to one another. For example:

- Component cables
- Electrical wires
- Ethernet cables
- WiFi
- Infrared signals

The art of connecting things is becoming more and more complex every day. Bluetooth can streamline the process. A Bluetooth connection is wireless and automatic, and it has a number of interesting features that can simplify our daily lives.

The Problem:

When any two devices need to talk to each other, they have to agree on a number of points before the conversation can begin. The first point of agreement is physical: Will they talk over wires, or through some form of wireless signals? If they use wires, how many are required -- one, two, eight, 25? Once the physical attributes are decided, several more questions arise:

How much data will be sent at a time? For instance, serial ports send data 1 bit at a time, while parallel ports send several bits at once.

How will they speak to each other? All of the parties in an electronic discussion need to know what the bits mean and whether the message they receive is the same message that was sent. This means developing a set of commands and responses known as a protocol.

Bluetooth offers a solution to the problem.

How Bluetooth Creates a Connection:

Bluetooth takes small-area networking to the next level by removing the need for user intervention and keeping transmission power extremely low to save battery power. Picture this: You're on your Bluetooth-enabled cell phone, standing outside the door to your house. You tell the person on the other end of the line to call you back in five minutes so you can get in the house and put your stuff away. As soon as you walk in the house, the map you received on your cell phone from your car's Bluetooth-enabled GPS system is automatically



Bluetooth wireless PC card

sent to your Bluetooth-enabled computer, because your cell phone picked up a Bluetooth signal from your PC and automatically sent the data you designated for transfer. Five minutes later, when your friend calls you back, your Bluetooth-enabled home phone rings instead of your cell phone. The person called the same number, but your home phone picked up the Bluetooth signal from your cell phone and automatically re-routed the call because it realized you were home. And each transmission signal to and from your cell phone consumes just 1 mill watt of power, so your cell phone charge is virtually unaffected by all of this activity.

Bluetooth is essentially a networking standard that works at two levels:

It provides agreement at the physical level -- Bluetooth is a radio-frequency standard.

It provides agreement at the protocol level, where products have to agree on when bits are sent, how many will be sent at a time, and how the parties in a conversation can be sure that the message received is the same as the message sent.

Advantages of Bluetooth:

The big draws of Bluetooth are that it is wireless, inexpensive and automatic. There are other ways to get around using wires, including infrared communication. Infrared (IR) refers to light waves of a lower frequency than human eyes can receive and interpret. Infrared is used in most television remote control systems. Infrared communications are fairly reliable and don't cost very much to build into a device, but there are a couple of drawbacks. First, infrared is a "line of sight" technology. For example, you have to point the remote control at the television or DVD player to make things happen. The second

drawback is that infrared is almost always a "one to one" technology. You can send data between your desktop computer and your laptop computer, but not your laptop computer and your PDA at the same time. (See [How Remote Controls Work](#) to learn more about infrared communication.)

These two qualities of infrared are actually advantageous in some regards. Because infrared transmitters and receivers have to be lined up with each other, interference between devices is uncommon. The one-to-one nature of infrared communications is useful in that you can make sure a message goes only to the intended recipient, even in a room full of infrared receivers.

Bluetooth is intended to get around the problems that come with infrared systems. The older Bluetooth 1.0 standard has a maximum transfer speed of 1 megabit per second (Mbps), while Bluetooth 2.0 can manage up to 3 Mbps. Bluetooth 2.0 is backward-compatible with 1.0 devices.

How Bluetooth Operates:

Bluetooth networking transmits data via low-power radio waves. It communicates on a frequency of 2.45 gigahertz (actually between 2.402 GHz and 2.480 GHz, to be exact). This frequency band has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM).

A number of devices that you may already use take advantage of this same radio-frequency band. Baby monitors, garage-door openers and the newest generation of cordless phones all make use of frequencies in the ISM band. Making sure that Bluetooth and these other devices don't interfere with one another has been a crucial part of the design process.

One of the ways Bluetooth devices avoid interfering with other systems is by sending out very weak signals of about 1 mill watt. By comparison, the most powerful cell phones can transmit a signal of 3 watts. The low power limits the range of a Bluetooth device to about 10 meters (32 feet), cutting the chances of interference between your computer system and your portable telephone or television. Even with the low power, Bluetooth doesn't require line of sight between communicating devices. The walls in your house won't stop a Bluetooth signal, making the standard useful for controlling several devices in different rooms.

Bluetooth can connect up to eight devices simultaneously. With all of those devices in the same 10-meter (32-foot) radius, you might think they'd interfere with one another, but it's unlikely. Bluetooth uses a technique called spread-spectrum frequency hopping that makes it rare for more than one device to be transmitting on the same frequency at the same time. In this technique, a device will use 79 individual, randomly chosen frequencies within a designated range, changing from one to another on a regular basis. In the case of Bluetooth, the transmitters change frequencies 1,600 times every second, meaning that more devices can make full use of a limited slice of the radio spectrum. Since every Bluetooth transmitter uses spread-spectrum transmitting automatically, it's unlikely that two transmitters will be on the same frequency at the same time. This same technique minimizes the risk that portable phones or baby monitors will disrupt Bluetooth devices, since any interference on a particular frequency will last only a tiny fraction of a second.

When Bluetooth-capable devices come within range of one another, an electronic conversation takes place to determine whether they have data to share or whether one needs to control the other. The user doesn't have to press a button or give a command -- the electronic conversation happens automatically. Once the conversation has occurred, the devices -- whether they're part of a computer system or a stereo -- form a network. Bluetooth systems create a personal-area network (PAN), or piconet, that may fill a room or may encompass no more distance than that between the cell phone on a belt-clip and the headset on your head. Once a piconet is established, the members randomly hop frequencies in unison so they stay in touch with one another and avoid other piconets that may be operating in the same room

Bluetooth Pico nets:

Most of the time, a network or communications method either works in one direction at a time, called half-duplex communication, or in both directions simultaneously, called full-duplex communication. A speakerphone that lets you either listen or talk, but not both, is an example of half-duplex communication, while a regular telephone handset is a full-duplex device. Because Bluetooth is designed to work in a number of different circumstances, it can be either half-duplex or full-duplex.

The cordless telephone is an example of a use that will call for a full-duplex (two-way) link, and Bluetooth can send data at more than 64 kilobits per second (Kbps) in a full-duplex link -- a rate high enough to support several voice conversations. If a particular use calls for a half-duplex link -- connecting to a computer printer, for example -- Bluetooth can transmit up to 721 Kbps in one direction, with 57.6 Kbps in the other. If the use calls for the same speed in both directions, Bluetooth can establish a link with 432.6-Kbps capacity in each direction.

Let's say you have a typical modern living room with typical modern stuff inside. There's an entertainment system with a stereo, a DVD player, a satellite TV receiver and a television; there's also a cordless telephone and a personal computer. Each of these systems uses Bluetooth, and each forms its own piconet to talk between the main unit and peripheral.

The cordless telephone has one Bluetooth transmitter in the base and another in the handset. The manufacturer has programmed each unit with an address that falls into a range of addresses it has established for a particular type of device. When the base is first turned on, it sends radio signals asking for a response from any units with an address in a particular range. Since the handset has an address in the range, it responds, and a tiny network is formed. Now, even if one of these devices should receive a signal from another system, it will ignore it since it's not from within the network. The computer and entertainment system go through similar routines, establishing networks among addresses in ranges established by manufacturers. Once the networks are established, the systems begin talking among themselves. Each piconet hops randomly through the available frequencies, so all of the piconets are completely separated from one another.

Now the living room has three separate networks established, each one made up of devices that know the address of transmitters it should listen to and the address of receivers it should talk to. Since each network is changing the frequency of its operation thousands of times a second, it's unlikely that any two networks will be on the same frequency at the same time. If it turns out that they are, then the resulting confusion will only cover a tiny fraction of a second, and software designed to correct for such errors weeds out the confusing information and gets on with the network's business.

Bluetooth Security:

In any wireless networking setup, security is a concern. Devices can easily grab radio waves out of the air, so people who send sensitive information over a wireless connection need to take precautions to make sure those signals aren't intercepted. Bluetooth technology is no different -- it's wireless and therefore susceptible to spying and remote access, just like WiFi is susceptible if the network isn't secure. With Bluetooth, though, the automatic nature of the connection, which is a huge benefit in terms of time and effort, is also a benefit to people looking to send you data without your permission.

Bluetooth offers several security modes, and device manufacturers determine which mode to include in a Bluetooth-enabled gadget. In almost all cases, Bluetooth users can establish "trusted devices" that can exchange data without asking permission. When any other device tries to establish a connection to the user's gadget, the user has to decide to allow it. Service-level security and device-level security work together to protect Bluetooth devices from unauthorized data transmission. Security methods include authorization and identification procedures that limit the use of Bluetooth services to the registered user and require that users make a conscious decision to open a file or accept a data transfer. As long as these measures are enabled on the user's phone or other device, unauthorized access is unlikely. A user can also simply switch his Bluetooth mode to "non-discoverable" and avoid connecting with other Bluetooth devices entirely. If a user makes use of the Bluetooth network primarily for synching devices at home, this might be a good way to avoid any chance of a security breach while in public.

Still, early cell-phone virus writers have taken advantage of Bluetooth's automated connection process to send out infected files. However, since most cell phones use a secure Bluetooth connection that requires authorization and authentication before accepting data from an unknown device, the infected file typically doesn't get very far. When the virus arrives in the user's cell phone, the user has to agree to open it and then agree to install it. This has, so far, stopped most cell-phone viruses from doing much damage. See [How Cell-phone Viruses Work](#) to learn more.

Other problems like "bluejacking," "bluebugging" and "Car Whisperer" have turned up as Bluetooth-specific security issues. Bluejacking involves Bluetooth users sending a

business card (just a text message, really) to other Bluetooth users within a 10-meter (32-foot) radius. If the user doesn't realize what the message is, he might allow the contact to be added to his address book, and the contact can send him messages that might be automatically opened because they're coming from a known contact. Bluebugging is more of a problem, because it allows hackers to remotely access a user's phone and use its features, including placing calls and sending text messages, and the user doesn't realize it's happening. The Car Whisperer is a piece of software that allows hackers to send audio to and receive audio from a Bluetooth-enabled car stereo. Like a computer security hole, these vulnerabilities are an inevitable result of technological innovation, and device manufacturers are releasing firmware upgrades that address new problems as they arise.

Difference between ZigBee and Bluetooth: -

ZigBee is broadly categorized as a low rate WPAN, and its closest technology is Bluetooth. A good bit of energy has been spent in analyzing whether ZigBee and Bluetooth are complementary or competing technologies, but after a quick look at the two, it can be seen that they fall a lot farther down the complementary side of the spectrum. They are two different technologies with very different areas of application and different means of designing for those applications.

- **Area of Application:**

While ZigBee is focused on control and automation, Bluetooth is focused on connectivity between laptops, PDA's, and the like, as well as more general cable replacement.

- **Data Rate:**

ZigBee uses low data rate, low power consumption, and works with small packet devices; Bluetooth uses a higher data rate, higher power consumption, and works with large packet devices.

- **Supportable Number of Devices:**

ZigBee networks can support a larger number of devices and a longer range between devices than Bluetooth.

- **Response Timing:**

In timing critical applications, ZigBee is designed to respond quickly, while Bluetooth takes much longer and could be detrimental to the application.

- **Battery Charging:**

As an example, for its applications, Bluetooth must rely on fairly frequent battery recharging, while the whole goal of ZigBee is for a user to be able to put a couple of batteries in the devices and forget about them for months to years.

Figure below shows a comparison of the various 802 technologies for data rate and range.

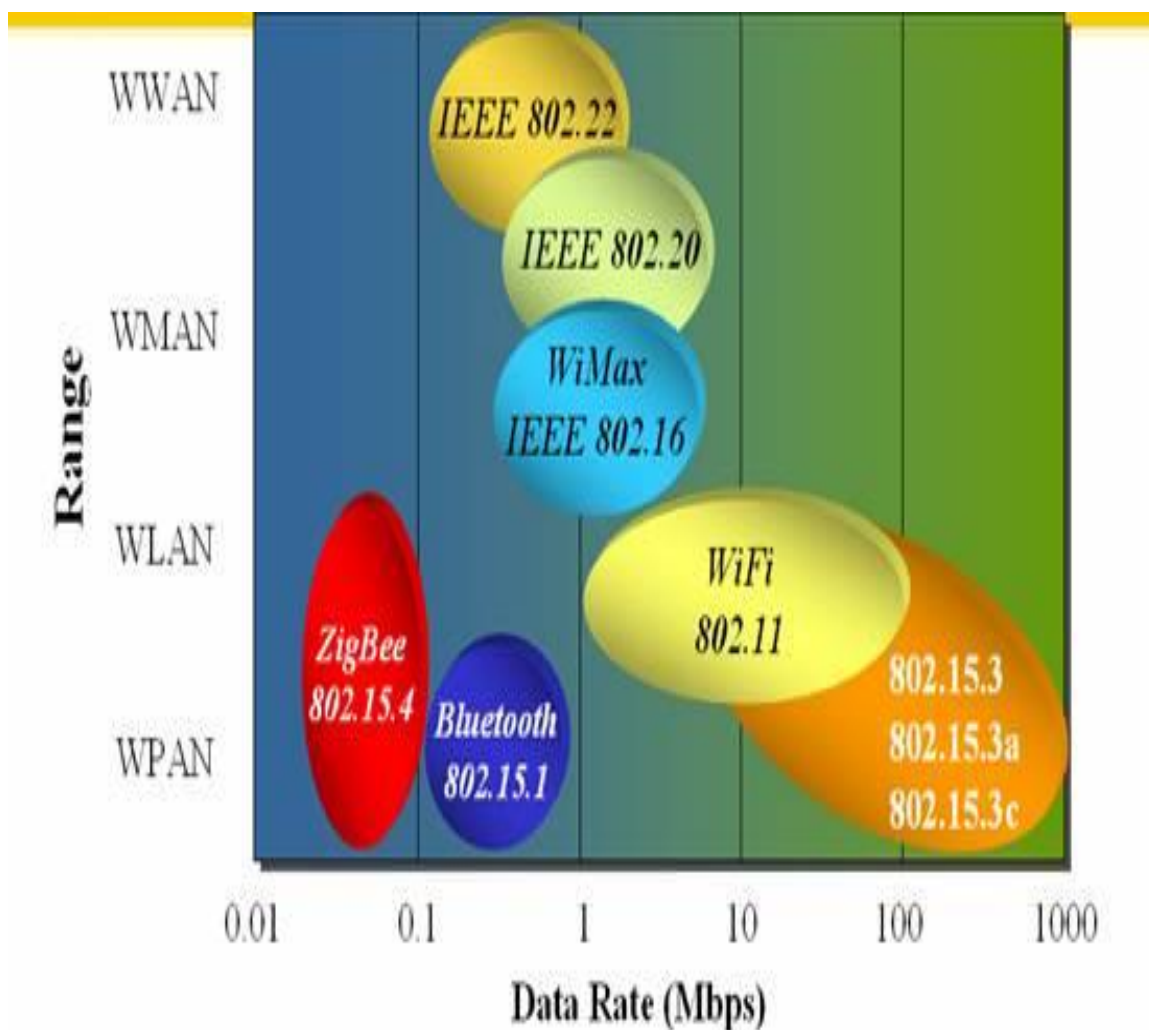


Figure 6: The 802 Wireless Space

	ZigBee	802.11 (Wi-Fi)	Bluetooth	UWB (Ultra Wide Band)	Wireless USB	IR Wireless
Data Rate	20, 40, and 250 Kbits/s	11 & 54 Mb/s/sec	1 Mb/s/s	100-500 Mb/s/s	62.5 Kbits/s	20-40 Kbits/s 115 Kbits/s 4 & 16 Mb/s/s
Range	10-100 meters	50-100 meters	10 meters	<10 meters	10 meters	<10 meters (line of sight)
Networking Topology	Ad-hoc, peer to peer, star, or mesh	Point to hub	Ad-hoc, very small networks	Point to point	Point to point	Point to point
Operating Frequency	868 MHz (Europe) 900-928 MHz (NA), 2.4 GHz (worldwide)	2.4 and 5 GHz	2.4 GHz	3.1-10.6 GHz	2.4 GHz	800-900 nm
Complexity (Device and application impact)	Low	High	High	Medium	Low	Low
Power Consumption (Battery option and life)	Very low (low power is a design goal)	High	Medium	Low	Low	Low
Security	128 AES plus application layer security		64 and 128 bit encryption			
Other Information	Devices can join an existing network in under 30ms	Device connection requires 3-5 seconds	Device connection requires up to 10 seconds			
Typical Applications	Industrial control and monitoring, sensor networks, building automation, home control and automation, toys, games	Wireless LAN connectivity, broadband Internet access	Wireless connectivity between devices such as phones, PDA, laptops, headsets	Streaming video, home entertainment applications	PC peripheral connections	Remote controls, PC, PDA, phone, laptop links

Table 1: Wireless Comparisons

Conclusion: -

Because of these differences, the technologies are not only geared toward different applications, they don't have the capability to extend out to other applications. Thus, a user could easily use both technologies as a wireless solution in a PAN to suit all types of applications within that network.



Sources:

- Bluetooth.com
<http://www.bluetooth.com>
- Bluetooth.org
<http://www.bluetooth.org>
- "Bluetooth Technology: What are the applications?" MobileInfo.com.
<http://www.mobileinfo.com/Bluetooth/applic.html>
- Fleishman, Glenn. "Inside Bluetooth 2.0." Macworld.com.
<http://www.macworld.com/news/2005/02/09/bluetooth2/index.php>
- Shepter, John. "How Bluetooth cuts the cord."
http://searchmobilecomputing.techtarget.com/generic/0,295582,sid40_gci1067872,00.html
- "Wireless Security." Bluetooth.com.
<http://www.bluetooth.com/help/security.asp>